Westvale Park
Primary Academy

Online Safety Policy

REVIEW: ANNUALLY **LAST REVIEW DATE: 10/9/25**

Key contacts

- Designated Safeguarding Lead
  Susan Kelly 01293 365019 skelly@westvaleppa.org.uk

- Deputy Safeguarding Lead
  Anica De Sa Pereira 01293 365019 adesapereira@westvaleppa.org.uk

- Deputy Safeguarding Lead
  Lorna Wilkinson 01293 365019 lwilkinson@westvaleppa.org.uk

- Deputy Safeguarding Lead
  Ryan Farrant 01293 365019 rfarrant@westvaleppa.org.uk

- Local Academy Board member with specific safeguarding responsibilities
  Ushma Olaitan) uolaitan@westvaleppa.org.uk

This policy will be reviewed **at least** annually. It will also be revised following any concerns and/or updates to national and local guidance or procedures.

Contents

1. Policy Aims

This Online Safety Policy has been developed by Westvale Park Primary Academy in consultation with staff, learners, the Local Academy Body (LAB) and parents/carers. It draws on the statutory guidance in:

- *Keeping Children Safe in Education (KCSIE), 2025*
- *Meeting Digital and Technology Standards in Schools and Colleges (DfE, 2024)*
- *Filtering and Monitoring Standards (DfE, 2024)*
- *Teaching Online Safety in Schools (DfE, 2023)*
- Surrey Safeguarding Children Partnership procedures
- UKCIS guidance, including *Sharing Nudes and Semi-Nudes* and *Education for a Connected World (2024 update)*

The purpose of this Online Safety Policy is to:

- Safeguard all members of the school community from online harm.
- Promote a whole-school culture that integrates online safety into safeguarding, behaviour, wellbeing and the curriculum.
- Support staff to work safely, professionally and confidently when using digital technology.
- Ensure learners build digital resilience and can recognise and manage online risks.
- Set clear procedures for responding to online safety incidents, ensuring concerns are recorded, escalated and acted upon appropriately.

Online safety risks fall into four key categories (KCSIE 2025):

1. Content – exposure to illegal, harmful or inappropriate material
2. Contact – harmful interaction with others online
3. Conduct – online behaviour that increases the risk of harm
4. Commerce/Contract – financial harm such as scams, phishing, gambling and sextortion

2. Policy Scope

Westvale Park Primary Academy recognises that online safety is a core part of safeguarding. The school has a duty to protect learners and staff from online harm, both in school and when using school-provided technology off-site.

This policy applies to:

- All staff (including LAB members, volunteers, contractors and visitors)
- All pupils
- Parents and carers

- Anyone using the school's digital technology, network, internet access or devices
- Personal devices being used on school premises or connected to the network

This policy covers all forms of digital communication or online activity, including:

- Use of school or personal devices
- Internet access, apps, email, learning platforms and social media
- Remote education and live-streaming
- Digital behaviour, image sharing, AI tools and online research

Under the Education and Inspections Act (2006) and Behaviour in Schools (DfE, 2024), the Headteacher may regulate pupil behaviour off-site and online where it impacts the school, another pupil, or staff member. The school will take reasonable and proportionate action where online behaviour outside school poses a safeguarding concern or breaches the Behaviour Policy.

2.1 Links With Other Policies

This Online Safety Policy links to and should be read alongside:

- WPPA – AAT - Safeguarding Policy
- Promoting Positive Behaviour & Wellbeing Policy
- Anti-Bullying Policy
- Acceptable Use Policies (staff and pupils)
- Staff Code of Conduct / AAT Staff Handbook
- RSE, PSHE and Computing curricula
- Confidentiality and Data Protection policies

2.2 Online Safety in Community Activities, After-School Clubs and Tuition

When school premises are hired to external organisations, Westvale Park ensures that these providers:

- Have appropriate safeguarding and child protection policies in place, including online safety
- Use suitable filtering and monitoring procedures
- Have a clear staff behaviour policy covering communication with children and families, including use of social media
- Are compliant with *Keeping Children Safe in Out-of-School Settings* (DfE)

- Are included in safeguarding agreements written into hire contracts or transfer-of-control agreements
- The school reserves the right to inspect policies and risk assessments before letting facilities.

3. Monitoring and Review

Because technology and online risks evolve rapidly, this policy will be:

- Reviewed at least annually
- Updated following changes in legislation, guidance, or digital standards
- Updated after any significant safeguarding incident or trend

The school will regularly monitor:

- Filtering and monitoring effectiveness
- Internet usage and emerging patterns of concern
- Staff and pupil understanding of online safety
- Use of devices and platforms across the curriculum

Oversight responsibilities:

- The Headteacher will be kept informed of online safety incidents and trends.
- The LAB member for safeguarding will receive regular reports and challenge senior leaders on compliance with the DfE and Surrey requirements.
- Findings from monitoring will feed directly into safeguarding action planning and staff CPD.

4. Roles and Responsibilities

The Designated Safeguarding Lead (DSL) for Westvale Park Primary Academy is:

Susan Kelly – Headteacher

Deputy DSLs are:

- Anica De Sa Pereira – Deputy Headteacher / SENCo
- Lorna Wilkinson – Emotional Literacy Support Assistant
- Ryan Farrant – Assistant Headteacher

All DSL functions remain the responsibility of the DSL (Susan Kelly) even when tasks are delegated.

The Local Academy Body (LAB) safeguarding lead is:

Ushma Olaitan – LAB Member for Safeguarding and Online Safety

We recognise that online safety is everyone's responsibility. All members of the school community have a role to play in creating a safe digital environment.

4.1 The Leadership and Management Team and LAB will:

- Treat online safety as a core safeguarding priority in line with *KCSIE 2025*.
- Ensure a whole-school approach to online safety, including behaviour, wellbeing, SEND, curriculum, pastoral systems and staff training.
- Ensure relevant policies—e.g. Behaviour, Safeguarding, AUPs - are consistent and interlinked.

Filtering & Monitoring (DfE Standards 2024)

- Ensure the school is fully compliant with the DfE Filtering and Monitoring Standards (2024).
- Assign a senior leader and LAB member (Ushma Olaitan) with explicit responsibility for meeting digital and online safety standards.
- Ensure filtering and monitoring systems are:
    - Age and stage appropriate
    - Reviewed at least annually
    - Understood by staff
    - Logged and monitored with clear escalation routes
- Evaluate the filtering and monitoring system with the DSL, technical staff and Wavenet/Smoothwall partner.

Curriculum and digital literacy

- Ensure that online safety is embedded as a progressive, preventative curriculum across Computing, PSHE, RSE and wider learning.
- Ensure teaching considers the specific needs of vulnerable children, including SEND, EAL, LAC and those with mental health needs.

Staff training

- Ensure all staff receive regular online safety training, including annual updates, that are integrated with safeguarding CPD.
- Ensure staff understand:
    - The four areas of online risk (content/contact/conduct/commerce)
    - Their responsibilities for safe online behaviour
    - How to report filtering breaches or online concerns

Oversight and accountability

- Ensure a culture of high expectations around professional digital conduct.
- Provide time and resources for DSL and deputy DSLs to fulfil online safety duties.
- Receive regular reports from the DSL on:
    - Online safety incidents
    - Trends/patterns
    - Filtering & monitoring checks
    - Curriculum developments
- Use this information to challenge and improve practice.

4.2 The Designated Safeguarding Lead (DSL) will:

(Susan Kelly – Headteacher)

Leadership responsibilities

- Take lead responsibility for online safety as part of safeguarding.
- Ensure online safety is considered across behaviour, attendance, SEND, pastoral support and teaching & learning.

Expertise and training

- Access regular advanced DSL training including:
    - Filtering & monitoring
    - Online child-on-child abuse
    - Youth-produced sexual imagery
    - Radicalisation
    - Digital harms and technology trends
- Keep up to date with national and Surrey SCP guidance.

Coordination across staff

- Work closely with:
    - Deputy DSLs
    - SENCo (Anica De Sa Pereira)
    - SLT
    - IT staff
- Ensure online safety is reflected in individual risk assessments and support plans.

Responding to concerns

- Oversee and quality assure all online safety incident responses (including sexting, harassment, cyberbullying, grooming, harmful content and filtering breaches).
- Consult with Surrey Police, C-SPA, LADO or CEOP when needed.

- Record all incidents accurately on safeguarding systems.

Monitoring and review

- Review filtering and monitoring logs and escalate concerns as appropriate.
- Analyse patterns to identify:
    - Vulnerable pupils
    - Emerging risks
    - Curriculum needs
- Use findings to adjust curriculum and staff CPD.

Community engagement

- Lead online safety communication with parents, including workshops, updates and guidance.
- Promote key national events such as Safer Internet Day.

Policy leadership

- Review the Online Safety Policy annually (minimum), involving staff, pupils and parents.
- Meet termly with LAB safeguarding lead (Ushma Olaitan).

4.3 Responsibilities of All Staff

All staff (including volunteers, support staff, contractors and supply staff) will:

Professional conduct and expectations

- Recognise that technology is central to many safeguarding risks and report concerns immediately.
- Read and follow this policy, Safeguarding Policy, Staff Code of Conduct and AUP.
- Model positive, safe and responsible online behaviour at all times.

Curriculum and classroom practice

- Embed online safety teaching in lessons wherever technology is used.
- Actively supervise pupils' online activity.
- Check websites, apps and digital tools for suitability before first use.

Reporting and escalation

- Understand how to report:
    - Filtering breaches
    - Harmful content

    - Online child-on-child abuse
    - Sexting/youth-produced imagery
    - Radicalisation concerns
- Follow the correct safeguarding pathways, including informing DSL promptly.

Privacy and security

- Keep data secure and follow GDPR expectations.
- Use only school systems for work communications.
- Lock/log out of devices when not in use.

4.4 Responsibilities of Technical Staff

Technical staff (internal or external) will:

- Support the DSL and leadership team to meet DfE digital, filtering and monitoring standards.
- Maintain secure systems, including:
    - Firewalls
    - Antivirus
    - Patch updates
    - Secure passwords
- Collaborate with the DSL on filtering and monitoring reviews.
- Immediately report filtering breaches or potential online risks.
- Ensure that monitoring alerts are escalated in line with safeguarding procedures.
- Provide transparency logs when requested by the DSL or leadership.

4.5 Responsibilities of Learners

Learners will be supported to:

- Read and follow the Acceptable Use Policy.
- Look after themselves and others online.
- Report anything worrying to a trusted adult.
- Use technology respectfully and responsibly.
- Understand their behaviour online can have offline consequences.
- Recognise unsafe content and know how to block/report.

4.6 Responsibilities of Parents and Carers

Parents and carers will be encouraged and expected to:

- Read the school's AUPs and support their child to follow them.
- Role-model safe and responsible online behaviour.
- Maintain oversight of their child's online activity at home.
- Engage with the school's online safety information and workshops.
- Report concerns to school when appropriate.
- Follow school expectations for digital conduct.

5. Education and Engagement Approaches

Westvale Park Primary Academy provides a comprehensive, progressive and preventative online safety curriculum. We recognise that effective online safety education builds digital resilience, supports positive wellbeing, and equips children with the skills to navigate online risks safely. Online safety is embedded across Computing, PSHE, RSE, the AAT Wellbeing Curriculum and wider school life.

5.1 Education and Engagement with Learners

We will:

Curriculum and teaching

- Deliver a sequenced online safety curriculum aligned to:
    - *Education for a Connected World (2024)*
    - *Teaching Online Safety in Schools (DfE, 2023)*
    - AAT Wellbeing Curriculum
    - Purple Mash Computing curriculum
    - Purple Mash 2BeSafe – Being safe in a digital world.
- Ensure children receive clear teaching before they use online tools or devices.
- Reinforce online safety during all lessons where technology is used.
- Help learners develop skills in:
    - Critical thinking
    - Evaluating online information
    - Understanding risks and consequences
    - Managing privacy and security
    - Recognising unsafe behaviour and harmful content
    - Safe use of AI tools and Chatbots

Digital literacy and critical thinking

We will teach pupils to:

- Check information sources for reliability.
- Understand how algorithms influence what they see online.
- Recognise bias, misinformation and persuasive techniques.
- Understand age restrictions on apps, games and social media.
- Use search engines safely and appropriately.

Child-friendly Acceptable Use

We will support learners to understand expectations by:

- Displaying age-appropriate AUP posters in all teaching spaces.
- Using simple, accessible language for KS1 and lower KS2.
- Teaching children what monitoring means and why it is used.
- Rewarding positive and safe digital behaviour.

Learner participation

We will:

- Gather pupil voice to shape online safety education.
- Include children in reviewing AUPs and classroom expectations.
- Encourage leadership roles—e.g. digital leaders—where appropriate.

Transition and preparation

We will provide increased online safety support during transition points, including:

- Year 6 → Year 7
  This includes lessons on privacy, online friendships, image sharing, gaming, and digital wellbeing.

External support

Where appropriate, we may work with:

- Surrey Police
- NSPCC
- Safer Internet Centre
- Childnet or similar training providers to enhance pupil understanding.

5.2 Vulnerable Learners

We recognise that some children are more vulnerable to online harm due to developmental, social, emotional or environmental needs. This includes (but is not limited to):

- Children with SEND
- Children with speech, language or communication needs
- Looked-after children
- Children with mental health needs
- Pupils with limited digital access, supervision or support at home
- Children with EAL

We will:

- Adapt teaching materials to meet individual needs.
- Teach vocabulary explicitly and scaffold understanding.
- Use social stories or visual resources where helpful.
- Work with the SENCo (Anica De Sa Pereira), DSL and pastoral team to tailor support.
- Consider individual risk assessments for those at higher risk.
- Provide additional adult modelling and guidance during online activities.

5.3 Training and Engagement with Staff

All staff play a crucial role in online safety education.

We will:

- Provide online safety induction for all staff and LAB members.
- Ensure all staff receive annual safeguarding training including online safety, with updates throughout the year.
- Provide staff with clear expectations for professional conduct online.
- Ensure staff know:
    - How to identify online risks
    - How to recognise signs of online harm
    - How to respond to concerns or incidents
    - How to escalate filtering breaches
    - How to support pupils in reporting and blocking

Professional competence

We will also:

- Offer training on safe use of AI tools and online platforms.

- Share recommended resources and guidance (Childnet, UKCIS, National Online Safety, etc.).
- Emphasise that all school systems are monitored and staff behaviour must remain professional.

5.4 Awareness and Engagement with Parents and Carers

We recognise that parents and carers have a crucial role in supporting safe online behaviour.

We will:

- Provide information through:
    - Workshops and webinars
    - Parent evenings
    - Newsletters and digital updates
    - Our school website
- Share guidance on:
    - Safe device use
    - Online gaming
    - Grooming and exploitation
    - Image sharing
    - Social media age restrictions
    - Managing screen time and digital wellbeing
- Explain how filtering and monitoring work in school.
- Explain how online safety is taught and what pupils are learning.
- Encourage parents to report concerns to school promptly.
- Share resources such as Internet Matters, CEOP, NSPCC, and the Surrey SCP website.

6. Responding to Online Safety Incidents and Concerns

Westvale Park Primary Academy recognises that online safety incidents can occur inside and outside school. All concerns relating to online harm will be taken seriously, recorded promptly and responded to using Surrey Safeguarding Children Partnership (SSCP) procedures.

We aim to create a culture where pupils feel confident reporting anything that makes them feel unsafe online.

Our community (staff, pupils, parents, volunteers) must:

- Know how to report an online safety concern
- Never investigate incidents themselves
- Follow school procedures at all times
- Maintain confidentiality and share information only with designated staff
- Record concerns promptly, accurately and factually

All online safety concerns must be passed to:

Susan Kelly – DSL (Headteacher) or Deputy DSLs: Anica De Sa Pereira, Lorna Wilkinson or Ryan Farrant

6.1 Concerns About Learners' Welfare

When a concern relates to the welfare or safety of a child, the DSL or Deputy DSL will:

- Follow the Safeguarding and Child Protection Policy
- Record the concern on the school's safeguarding system immediately
- Consider the level of need using the SSCP Threshold Document
- Refer to Children's Services via the C-SPA if needed (Levels 3–4)
- Consult with external agencies (e.g., Surrey Police, CEOP) where appropriate
- Inform parents/carers unless doing so places a child at increased risk

Examples of incidents that must be reported:

- Cyberbullying, harassment or online threats
- Exposure to harmful or age-inappropriate content
- Online grooming concerns
- Youth-produced sexual imagery ("sexting")
- Online sexual harassment
- Radicalisation/extremist content
- SCAMS, phishing, fraud or sextortion attempts
- Concerns about a child's digital wellbeing (dependency, sleep issues, distress)

The DSL will provide appropriate support for all children involved, including pastoral, restorative, and wellbeing support.

6.2 Staff Misuse

Any allegation or concern about staff online conduct must be reported to:

Susan Kelly – Headteacher (or in cases involving the Headteacher, directly to the Chair of LAB)

Examples include:

- Inappropriate communication with pupils
- Sharing or accessing inappropriate content
- Breaching staff AUP or Code of Conduct
- Using personal devices unprofessionally
- Behaviour that could constitute grooming or abuse

The school will:

- Follow the AAT Allegations Against Staff Policy
- Seek immediate advice from the Local Authority Designated Officer (LADO)
- Involve Surrey Police where a potential offence has occurred
- Take proportionate actions while following due process

Staff must never attempt to view or handle illegal content themselves.

7. Procedures for Responding to Specific Online Incidents or Concerns

7.1 Child-on-Child Online Sexual Violence and Sexual Harassment

Westvale Park Primary Academy follows Part 5 of KCSIE 2025, which makes clear that child-on-child sexual violence or harassment can occur online and must always be taken seriously.

Examples include:

- Non-consensual sharing of nudes/semi-nudes
- Sharing sexualised images or videos of others
- Sending unwanted sexual messages
- “Upskirting” or voyeuristic content
- Threatening to share sexual content
- Sexualised comments in chats, games or group messages

If an incident is reported:

The DSL or Deputy DSL will:

1. Act immediately and follow the Child Protection Policy.
2. Listen to the child, not question or blame.
3. Assess the nature and level of risk to all children involved.
4. Consider the need for police involvement (Surrey Police 101 / 999).
5. Secure devices where necessary, following DfE Searching, Screening & Confiscation guidance.
6. Provide immediate, proportionate support to the victim(s).
7. Implement appropriate disciplinary action for perpetrators in line with the Behaviour and Anti-Bullying Policies.
8. Inform parents/carers where appropriate.
9. Work with other schools if children from different settings are involved.

We will take steps to prevent further harm, including blocking/reporting content, removing access, and supporting digital resilience.

7.2 Youth-Produced Sexual Imagery ("Sharing Nudes and Semi-Nudes")

We follow UKCIS (2023) "Sharing Nudes and Semi-Nudes" guidance.

Key principles:

- All incidents must be reported to the DSL
- Staff must not view the imagery unless absolutely necessary to safeguard
- Staff must never copy, share, or store imagery
- The DSL makes the decision on whether to:
    - Manage internally
    - Refer to C-SPA
    - Inform the police
    - Take other safeguarding action

DSL actions include:

- Risk assessment of the situation
- Securing devices (without opening files)
- Checking if the image is on the school network and isolating it
- Supporting pupils involved, including using Report Remove tools
- Informing parents/carers if appropriate

- Keeping accurate records
- Deleting imagery only when police confirm it is lawful to do so

7.3 Online Child Sexual Abuse and Exploitation (Including Criminal Exploitation and County Lines)

This includes:

- Online grooming
- Live streaming abuse
- Sextortion (sexual extortion)
- Children coerced to perform sexual acts online
- Attempts to involve children in criminal activity (drug distribution, fraud, etc.)

The DSL will:

- Refer immediately to C-SPA
- Contact Surrey Police
- Secure any device/evidence safely
- Provide support for the child
- Work with CEOP where needed

Ensure risks to siblings or other pupils are considered

7.4 Indecent Images of Children (IIOC)

If IIOC is found on any device:

- DSL must be informed immediately
- Staff must not view or share the content
- The DSL will contact:
    - Surrey Police
    - Internet Watch Foundation (IWF)
    - LADO, if a staff member may be involved
- Devices will be quarantined
- URLs and digital locations will be reported to IWF
- The school will ensure all safeguarding and legal processes are followed

The DSL will also ensure emotional and wellbeing support is provided.

7.5 Cyberbullying

- Cyberbullying will be treated with the same seriousness as offline bullying.
- See Anti-Bullying Policy for full details.

7.6 Cybercrime

Some pupils with advanced computing skills may unintentionally or deliberately commit cyber-dependent crimes such as:

- Hacking
- DDoS attacks
- Malware creation
- Accessing secure data

Where concerns arise:

- DSL may consult Cyber Choices programme
- Surrey Police may be contacted for advice
- Support and education will be provided to the pupil

7.7 Online Hate

Online hate incidents include racial, homophobic, sexist, ableist or discriminatory content.

We will:

- Record and respond to incidents in line with the Behaviour Policy
- Report to police if a crime may have been committed
- Provide support for targeted pupils
- Educate pupils about respect and equality online

7.8 Online Radicalisation and Extremism

We follow the Prevent Duty and KCSIE 2025.

If content or behaviour raises a radicalisation concern:

- DSL will act immediately
- Channel or Prevent referrals may be made
- Surrey Police Prevent team may be contacted
- Filtering systems are reviewed to ensure extremist content is blocked
- The child is supported with proportionate intervention

8. Safer Use of Technology

Westvale Park Primary Academy is committed to using technology in a way that enhances learning while keeping pupils and staff safe. All technology use is framed through safeguarding, data protection, cyber security, and professional conduct expectations.

This section outlines how the school ensures safe, secure and responsible use of digital tools, devices, platforms, and online services.

8.1 Classroom Use

We use a wide range of digital tools and devices including laptops, desktops, tablets, cameras, learning platforms and online content.

All classroom use must:

- Follow the school's Acceptable Use Policies
- Follow the Behaviour and Safeguarding policies
- Be supervised appropriately at all times
- Enhance learning and align to planned curriculum outcomes

Staff responsibilities:

- Pre-check websites, apps, videos or AI tools before use
- Ensure content is age-appropriate and safe
- Remind pupils of expectations before going online
- Actively monitor screens, including when pupils are working independently
- Immediately report unsuitable sites or content to the DSL and technical staff
- Model safe behaviour (privacy, copyright, respectful conduct)
- *Staff will not use generative AI tools with pupils unless risk assessed and approved by SLT.*
- *Staff must not input personal data, pupil work, or identifiable pupil information into AI systems.*
-

Search tools and internet access:

- Children will use **age-appropriate search engines**, child-safe filters or curated links
- Google Safe Search will be enabled on all devices

- Early Years & Key Stage 1:
    - Primarily access the internet through staff demonstration
    - Occasional, closely supervised access for specific learning tasks
- Key Stage 2:
    - Use the internet independently with direct supervision
    - Taught how to search safely and evaluate content

Use of AI and chatbots:

When AI tools are used for learning, staff will:

- Pre-assess risk
- Ensure no personal data about a child is entered
- Teach pupils how to use AI critically and responsibly

The goal is to prepare children for a digital world while managing risks carefully.

8.2 Managing Internet Access

To keep pupils and staff safe online, we will:

- Maintain an accurate record of everyone with access to the school's devices and network
- Require all staff, visitors, governors and pupils to sign an AUP before network access is granted
- Ensure visitors use guest-access systems that prevent access to school data
- Ensure internet access is logged and monitored in accordance with data protection legislation

The school reserves the right to restrict or withdraw access if there is a safeguarding risk.

8.3 Filtering and Monitoring

Westvale Park Primary Academy is **fully compliant** with the **DfE Filtering and Monitoring Standards 2024**, which are mandatory expectations for all schools.

This includes annual review and ongoing oversight by senior leaders and LAB members.

8.3.1 Decision Making

Our filtering and monitoring systems are designed to:

- Reduce exposure to harmful content
- Protect learners from extremist, illegal or abusive material
- Support safeguarding responses through effective monitoring alerts
- Prevent over-blocking so that learning is not unnecessarily restricted
- Meet the needs of different age groups and curriculum contexts

Leadership responsibilities:

- Termly review of filtering and monitoring with:
    - DSL (Susan Kelly)
    - Technical staff
    - LAB Safeguarding Lead (Ushma Olaitan)
    - Wavenet/Smoothwall provider
- Risk assessment of any proposed filtering changes
- Logging and recording all adjustments to filtering settings
- Ensuring staff know:
    - What is blocked
    - What is monitored
    - How to report breaches
- Ensuring policies reflect current filtering/monitoring arrangements
- Ensuring parents know how technology is monitored at school

Filtering must not be the only safeguarding measure — education, supervision and culture remain essential.

8.3.2 Technical Systems in Use

The school uses:

- **Wavenet** for broadband connectivity
- **Smoothwall** for filtering and monitoring

Smoothwall automatically blocks:

- Illegal content (IIOC, extremist content)
- Sites on the Internet Watch Foundation (IWF) list
- Sites on the Counter Terrorism Internet Referral Unit (CTIRU) list
- Adult content

- Gambling
- High-risk categories such as anonymous browsing, hacking, weapons and hate content

When a pupil encounters unsuitable content:

They should:

1. Immediately turn off the screen
2. Report it to the supervising adult

Staff must then:

- Record the URL if known
- Report to the DSL and technical team
- Ensure appropriate logs are updated
- Inform parents where relevant
- Seek police advice where content may be illegal

8.3.3 Monitoring

Monitoring includes:

- Supervision by staff
- Logfile and internet usage review
- Smoothwall monitoring alerts (daily to DSL)
- Keyword alerts linked to safeguarding themes such as:
    - Self-harm
    - Suicide
    - Bullying
    - Radicalisation
    - Grooming
    - Violence
    - Sexual content

All users are informed that:

- Use of school devices is monitored
- Monitoring is proportionate, lawful and aligned with GDPR
- Logs may be shared with police where required

Where a monitoring alert is generated:

- DSL/Deputy DSLs review the alert
- Safeguarding action is taken if necessary

- Patterns and trends are analysed termly

8.4 Managing Personal Data Online

Personal data must always be handled safely and lawfully.

Full information can be found in our Trust Data Protection Policy.

We follow:

- UK GDPR
- Data Protection Act 2018
- AAT Data Protection and Retention Policies
- DfE Cyber Security Standards (2024)

We ensure:

- Staff use secure systems for storing and sharing data
- Only authorised personnel can access sensitive information
- Personal data is never entered into AI tools or unapproved apps
- Staff understand how to identify and report data breaches.

8.5 Security and Management of Information Systems

We meet the DfE Cyber Security Standards for Schools and Colleges (2024).

We ensure:

- All devices have firewalls and antivirus protection
- Security updates are applied promptly
- Strong passwords and access controls are used
- Staff accounts only allow access needed for their role
- No unapproved software or apps are downloaded
- Portable media (e.g. USBs) are not used unless encrypted and approved
- Activity on the network is monitored for inappropriate use or misuse
- Staff lock their screens or log out when unattended

8.5.1 Password Policy

Staff must:

- Use strong, complex passwords
- Keep passwords private
- Change passwords annually
- Use 2-factor authentication on all sensitive accounts
- Never log in as another user

Staff are responsible for the security of their accounts.

Pupils at Westvale Park Primary Academy use Wonde MyLogin to access school Chromebooks and key learning platforms. Each child is given a unique six-emoji password, which provides secure single sign-on to:

- Times Tables Rock Stars
- Numbots
- Accelerated Reader
- Purple Mash

Emoji passwords are age-appropriate, easy to remember, and reduce the need for written passwords.
Teachers ensure pupils keep their emoji passwords private and support them to log in safely and independently.

8.6 Managing the Safety of our Website

Our school website must comply with DfE requirements.

We ensure:

- No personal staff or pupil information is published
- Contact details are generic school details only
- Website content meets accessibility standards
- Website admin accounts use strong passwords
- Safeguarding and online safety information is clearly published
- All copyrighted material is used legally

8.7 Publishing Images and Videos Online

We follow AAT Image Use, Data Protection and Safeguarding policies.

Staff must:

- Only use school devices to take photos/videos
- Never use personal devices
- Obtain parental consent prior to publication
- Use images respectfully and appropriately
- Never name individual children alongside images

The DSL will oversee any concerns about image use.

8.8 Managing Email

General expectations:

- School email accounts must be used for school communication
- Staff email is monitored in line with GDPR
- Staff should not email pupils directly unless authorised
- Sensitive information must be sent securely and encrypted
- Spam/Junk mail must be reported and not opened
- Chain messages and mass forwards are prohibited

Staff email expectations:

- Do not respond to emails outside professional hours (suggested cut-off 6pm)
- Maintain professional tone and confidentiality
- Do not set up accounts for apps/social media using staff email

Pupil email expectations:

- KS2 pupils use school-provided email only for learning (Purple Mash)
- EYFS/KS1 may use class or group email accounts
- Pupils will be taught safe email etiquette

Email use will be monitored by staff

8.9 Live Stream Lessons for Remote Learning

Updated to current DfE expectations (post-COVID)

Live-streamed sessions may be used for:

- Remote learning (rare occasions)
- SEND support
- Pastoral/wellbeing sessions
- Virtual workshops or external provision

Safeguarding controls:

- Two members of staff present in the online room
- Sessions must be planned and approved by SLT
- Staff must use school devices and accounts
- Sessions recorded where appropriate, following data protection requirements
- Children must attend from a suitable space (not bedrooms where possible)
- Pupils must be appropriately dressed
- No one may record, screenshot or share the session

Platform risk assessment includes:

- Chat/comment functions
- Camera use
- Private messaging options
- Recording features
- Screen-sharing permissions

1:1 sessions:

Only permitted for:

- Counselling
- Mental health support
- SEND intervention
- Behaviour support

Requirements:

- Parent consent
- Two staff in the call or visible/audible oversight
- Clear safeguarding protocols
- DSL oversight

8.10 Management of Learning Platforms

We use **Purple Mash** as our main learning platform.

We ensure:

- Only current staff, pupils and authorised parents can access
- Accounts are removed when individuals leave
- Content uploaded is appropriate and follows copyright laws
- Staff monitor communication tools within the platform
- Inappropriate content is removed quickly and logged
- Parents are informed when necessary

Visitors may only be given access where authorised by SLT.

8.11 Management of Applications (Apps) Used to Record Children's Progress

We use:

- **Tapestry** for EYFS
- **Provision Mapper** for SEND

We ensure:

- Only school devices are used
- Staff do not access apps from personal devices
- Devices are encrypted
- Passwords are strong and secure
- Parents understand expectations for their own access
- Data is stored and shared in accordance with GDPR

The EYFS Lead, SENCo and DSL oversee access and data security.

9. Social Media

Social media is a part of everyday life for many members of our school community. This section sets out clear expectations to ensure that social media is used positively, safely and responsibly by staff, pupils, parents and the school itself.

"Social media" includes (but is not limited to): blogs, wikis, forums, messaging apps, video-sharing

platforms, livestreaming services, gaming chats, social networking sites, discussion boards, comment sections, and any digital space where people interact or publish content.

Our aim is to protect the reputation, safety and wellbeing of pupils, staff and Westvale Park Primary Academy.

9.1 Expectations (All Members of the Community)

All members of Westvale Park Primary Academy must:

- Use social media respectfully, safely and responsibly
- Never post content that is threatening, hurtful, defamatory or discriminatory
- Maintain confidentiality and protect personal information
- Respect the rights, dignity and privacy of others
- Not share images or videos of pupils (other than their own child where permissions allow)
- Not post content that could harm the reputation of the school or individuals within it

While on school premises or using school-provided devices:

- Social media use is restricted to break times for staff
- Filtering and monitoring systems may restrict access
- Access to social media during learning time is prohibited for pupils unless explicitly part of a supervised lesson

Concerns or allegations:

Any concern about inappropriate online behaviour—including rumours, harassment, incitement, abuse or reputational damage—must be reported to the DSL or Deputy DSLs

9.2 Staff Personal Use of Social Media

Staff behaviour online must meet the same professional standards expected offline.

Professional conduct

Staff must:

- Uphold the reputation of the school at all times
- Never post content that could bring the profession into disrepute
- Maintain strong privacy settings
- Use two-factor authentication where available
- Avoid posting personal opinions that could undermine professional integrity
- Never identify themselves as employees of Westvale Park to express personal views

Separation of personal and professional life

Staff should:

- Not accept or invite “friend” requests from current or former pupils
- Not communicate with pupils or parents via personal accounts
- Not join group chats involving parents or pupils
- Not comment on school issues, decisions or incidents online
- Use school email/accounts for all school communication

If there is a pre-existing family relationship with a pupil, staff must inform the DSL and SLT.

Protecting privacy

Staff must:

- Keep personal accounts private
- Restrict location-sharing
- Log out of devices after use
- Not share photos or information about school activities on personal profiles

Reporting concerns

Staff must report:

- Any contact from pupils or parents on personal accounts
- Any reputational damage to themselves or the school
- Any safeguarding concerns arising from online behaviour

9.3 Learners’ Personal Use of Social Media

While most major platforms require users to be **13+** (WhatsApp **16+**), younger pupils may still attempt to access them.

We will educate pupils about:

- Age restrictions
- Privacy settings
- Blocking and reporting
- Respectful communication
- Avoiding oversharing
- Digital footprints
- Online pressures, comparison and wellbeing
- How algorithms influence what they see

- Recognising grooming, scams and manipulation

The school will:

- Address issues arising from pupils' use of social media—even if it occurs off-site—where it impacts the school community
- Inform parents of incidents
- Apply appropriate consequences in line with the Behaviour Policy
- Support victims of online bullying or harassment

Pupils are taught not to:

- Add or communicate with strangers
- Share images or videos of themselves or others unsafely
- Join group chats with unknown individuals
- Respond to harmful messages
- Use school systems to access social media unless appropriate as part of curriculum

9.4 Official Use of Social Media (School Accounts)

Westvale Park Primary Academy may use social media to:

- Share learning and celebrate achievements
- Communicate with families
- Promote school events and values
- Strengthen community relationships

When using official accounts:

- Posts must be professional, factual and aligned with school values
- No personal opinions will be shared
- All content must be respectful, positive and appropriate
- Confidential or sensitive information must never be shared

Safeguarding and GDPR

- No full names of pupils will be used
- Images will only be posted with parental consent
- Staff managing accounts will use school logins only
- SLT must approve account creation and high-risk posts
- Only authorised staff will have access to login details

Oversight and moderation

- Leadership team will have access to all accounts
- Comments will be monitored and moderated regularly
- Inappropriate comments may be removed or reported
- Users who repeatedly breach expectations may be blocked

Boundary between staff and school accounts

If staff choose to follow/like the official school account, they are encouraged to do so through **professional profiles** rather than personal ones.

Engagement with pupils and parents

Staff must not:

- Message parents or pupils via school social media
- Respond to personal messages (direct them to appropriate channels)
- Engage in disputes or complaints online

10. Use of Personal Devices and Mobile Phones

Westvale Park Primary Academy recognises that mobile phones and personal devices are part of modern life. However, they can present significant safeguarding, privacy, and data protection risks if not managed appropriately.

Our aim is to maintain a safe and respectful learning environment where the welfare of pupils and staff is prioritised.

This policy applies to:

- Staff
- Pupils
- Parents/carers
- Visitors, contractors and volunteers
- Anyone on school premises or participating in school activities

“Personal devices” include mobile phones, smartwatches, tablets, cameras, laptops, USBs and any device capable of storing or transmitting data.

10.1 Expectations (All Members of the Community)

Everyone must:

- Use devices responsibly, safely and legally
- Follow all school policies including Safeguarding, AUP, Behaviour and Data Protection
- Ensure devices do not disrupt learning or compromise safety
- Not record, photograph or film on school premises unless authorised
- Not share images or information about pupils (other than their own child where permissions allow)

Devices are not permitted in:

- Classrooms
- Toilets
- Playgrounds
- Any pupil-only area

(Staff are permitted to use devices in the staffroom, offices, and designated adult-only spaces.)

Unauthorised use may result in:

- Confiscation
- Behaviour consequences
- Restriction of privileges
- Removal of access rights
- Contact with parents
- Police involvement for illegal content

10.2 Staff Use of Personal Devices and Mobile Phones

Staff must be exemplary role models in their use of technology.

Staff must:

- Keep personal devices out of sight and on silent during lesson time
- Store devices securely (staffroom lockers, drawers, office spaces)
- Not use personal devices to contact pupils or parents
- Not use personal devices for taking photos/videos of pupils
- Use school devices for all work-related digital activity
- Not access social media during teaching time
- Not use Bluetooth/Airdrop in school areas accessible to pupils
- Follow data protection and confidentiality expectations at all times

Permitted use:

- Personal phone use during breaks, in staff-only areas
- Emergency contact when authorised by SLT

If a staff member needs to be contactable (e.g. medical or family emergency):

- This must be agreed with SLT
- Device must remain discreet and usage limited

Breaches:

Any misuse will be managed under the Staff Code of Conduct and, where necessary, may be referred to the LADO or police.

10.3 Learners' Use of Personal Devices and Mobile Phones

Westvale Park Primary Academy has a clear, consistent and child-centred approach to pupil mobile phone use.

Our school policy:

- Only Year 5 and Year 6 pupils who walk home independently may bring a phone to school
- Phones must be switched off on arrival and handed into the school office
- Phones are stored securely and collected at the end of the day
- Phones must not be used on site at any time

All other year groups:

- **Mobile phones are not permitted**, including for pupils who do not walk home unaccompanied – unless medically required.

Smartwatches:

- Not permitted in school
- Simple wristwatches without connectivity are acceptable

Mobile data:

- Use of 3G/4G/5G is strictly prohibited on site
- Pupils may not “hotspot” other devices

If a pupil needs to contact home:

- They may request to use the office telephone

- Parents wishing to contact their child must phone the school office

Misuse includes:

- Having a device without permission
- Using devices on site
- Taking photos/videos
- Contacting others during the day
- Online bullying or inappropriate communication
- Searching or viewing inappropriate content

Sanctions for misuse:

- Immediate confiscation
- Device returned only to parent/carer
- Behaviour consequences in line with the Behaviour Policy
- Repeated misuse may result in the child losing permission to bring a phone
- Illegal content will be reported to Surrey Police

Searching, screening and confiscation (DfE 2023):

- A senior leader may search a phone/device
- Consent from the pupil or parent is sought where possible
- Staff will never search through personal accounts unless legally required
- Illegal or harmful content will be handed to police immediately

Supporting Pupils with Medical Conditions

In line with the ***Supporting Pupils with Medical Conditions*** statutory guidance, Westvale Park Primary Academy recognises that some pupils with Type 1 Diabetes may require the use of a mobile phone linked to their medical device to manage their condition safely during the school day.

Where a mobile phone is medically required (e.g., to operate a continuous glucose monitor, insulin pump, food-logging app, or to receive high/low glucose alerts):

• The device is permitted only with a signed Individual Healthcare Plan (IHP) agreed by parents, the school and the Diabetes Team
• The phone must be used solely for medical purposes and kept in a location agreed in the IHP (e.g., medical room, class medical box, or carried by the pupil where clinically essential)
• Any alarms (high/low glucose alerts) may sound when medically necessary; staff will follow the child's IHP
• The device must not be used for messaging, calls, photos, social media, games or general internet access
• Mobile data and all non-medical notifications must be disabled
• Staff will supervise use as appropriate and support the pupil to respond to alarms safely and discreetly

• Misuse of the device, or any use not related to medical need, will be addressed in line with safeguarding and behaviour procedures

10.4 Visitors' Use of Personal Devices and Mobile Phones

Visitors (including volunteers, contractors and external professionals) must follow safeguarding expectations.

Visitors must not:

- Use phones or devices in classrooms, corridors or playgrounds
- Take photos/videos of pupils
- Record conversations or interactions
- Access social media while on school premises

Visitors may:

- Use phones in designated areas (reception, meeting rooms, car park)
- Use school Wi-Fi only when authorised

Staff responsibilities:

- Challenge visitors using devices inappropriately
- Report concerns to DSL/Deputy DSL

All visitors are informed of expectations through:

- Signage
- Visitor badges
- Verbal briefing at sign-in

11. Useful Links for Educational Settings

Statutory Guidance

- **Keeping Children Safe in Education (KCSIE, 2025)**
- **Filtering and Monitoring Standards for Schools and Colleges (DfE, 2024)**
- **Meeting Digital and Technology Standards in Schools and Colleges (DfE, 2024)**
- **Searching, Screening and Confiscation (DfE, 2023)**
- **Behaviour in Schools Guidance (DfE, 2024)**
- **Teaching Online Safety in Schools (DfE, 2023)**
- **Prevent Duty Guidance (Home Office, updated)**

National Support and Reporting

- **CEOP** – Report online abuse
- **UK Safer Internet Centre (UKSIC)** – Advice and professional resources
- **Internet Watch Foundation (IWF)** – Report or remove illegal images
- **NSPCC** – Child protection advice
- **Childline** – Support for children
- **National Online Safety** – Online safety parent guides
- **Cyber Choices (NCA)** – Preventing cybercrime

Guidance from UKCIS

- *Education for a Connected World (2024)*
- *Sharing Nudes and Semi-Nudes (2023)*
- *Social Media and Mental Health Guidance*

Local Support

- **Surrey Safeguarding Children Partnership (SSCP)** – Local procedures, thresholds and advice
- **C-SPA (Children's Single Point of Access)** – Referrals and safeguarding concerns
- **Surrey Police** – Non-emergency and online harm reporting

Positive Digital Use

- **Internet Matters** – Family online safety support
- **Thinkuknow** – Age-appropriate learning activities
- **Childnet** – Resources for schools and families
- **BBC Own It** – Digital wellbeing for children

These links will be reviewed annually to ensure accuracy and relevance.

12. Related Policies

This Online Safety Policy should be read alongside (but not limited to) the following school and AAT trust-wide policies:

Safeguarding and Protection

- Safeguarding and Child Protection Policy
- Prevent Duty Procedures
- Allegations Against Staff (AAT)

Behaviour, Conduct and Wellbeing

- Behaviour and Positive Relationships Policy
- Anti-Bullying Policy
- Mental Health and Wellbeing Policy
- Staff Code of Conduct (AAT)

Technology, Privacy and Data

- Data Protection and GDPR Policy
- Image Use Policy
- Mobile Phone and Personal Devices Policy
- Acceptable Use Policies (AUPs):
    - Staff
    - Pupils (EYFS/KS1)
    - Pupils (KS2)
    - Visitors
    - Volunteers

Curriculum Documentation

- Computing Curriculum
- PSHE & RSE Curriculum
- AAT Wellbeing Curriculum
- Remote Learning Policy (if applicable)

Operational / Pastoral

- Attendance Policy
- Inclusion / SEND Policy
- Educational Visits Policy

- Complaints Policy

Site and Access

- Visitor Policy
- Health & Safety Policy

All associated documents will be reviewed in line with the Online Safety Policy to maintain consistency and ensure a coherent safeguarding culture.

13. Disclaimer